Réciprocité quadratique, preuve de Zolotareff

Dominique Hoareau, domeh@wanadoo.fr

On énonce le théorème le plus célèbre de la Théorie des Nombres, la fameuse loi de réciprocité quadratique, démontré pour la première fois par Gauss en 1796. La preuve proposée ici est due à Zolotareff (1872) et s´appuie essentiellement sur des calculs de signatures de permutations. Une des difficultés de la démonstration est de s´assurer du caractère exhaustif de l´énumération des inversions. Ce thème est aussi un prétexte pour revoir quelques "joyaux de l'arithmétique" comme le petit théorème de Fermat ou la congruence de Wilson.

Référence : *Algorithmes algébriques*, Naudé,Quitté, Masson.

A- Signature d´une permutation

I désigne un ensemble fini de cardinal n, $\mathcal{S}_I$ le groupe des permutations de I (qui est engendré par les transpositions). Si on munit I d´un ordre total et si σ est une permutation de I, on appelle inversion de σ tout couple (i, j) de $I \times I$ tel que $i < j$ et $\sigma(i) > \sigma(j)$. On note $N(\sigma)$ le nombre d´inversions de σ.

Signature sur $\mathcal{S}_n$
Lorsque I est l´ensemble $[[1, n]] = \{1, 2, .., n\}$, on considère la relation d´ordre induite par l´ordre naturel sur $\mathbb{N}$ et on pose, pour σ dans $\mathcal{S}_n$, $\varepsilon(\sigma) = (-1)^{N(\sigma)}$. On a, par exemple, $\varepsilon(\sigma) = -1$ dès que σ est une transposition. On montre que ε est un morphisme de groupes de $\mathcal{S}_n$ sur $\{-1, 1\}$. On peut vérifier que la signature d´un cycle de longueur l est $(-1)^{l-1}$.

Signature sur $\mathcal{S}_I$
Soit $\sigma \in \mathcal{S}_I$. Si ϕ et ψ sont deux bijections de $[[1, n]]$ sur I, on montre que les deux permutations $\phi^{-1} \circ \sigma \circ \phi$ et $\psi^{-1} \circ \sigma \circ \psi$ de $\mathcal{S}_n$ ont la même signature. On pose alors légitimement : $\varepsilon(\sigma) = \varepsilon(\phi^{-1} \circ \sigma \circ \phi)$ où ϕ est une bijection quelconque de $[[1, n]]$ sur I. Si on énumère les éléments de I sous la forme $\phi(1), \phi(2), .., \phi(n)$, on définit un ordre total sur I : $i < j$ signifie i précède j dans la liste ci-dessus. On vérifie que $N(\sigma)$ pour l´ordre attaché à ϕ est égal au nombre d´inversions de $\phi^{-1} \circ \sigma \circ \phi$ pour l´ordre usuel sur $[[1, n]]$. La parité de $N(\sigma)$ est donc indépendante de l´ordre choisi sur I et on a : $\varepsilon(\sigma) = (-1)^{N(\sigma)}$. Lorsque les éléments de I appartiennent à un corps commutatif, $\varepsilon(\sigma)$ s´écrit aussi : $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$. Avec l´isomorphisme de groupes $\sigma \mapsto \phi^{-1} \circ \sigma \circ \phi$ de $\mathcal{S}_I$ sur $\mathcal{S}_n$, on montre que l´application $\varepsilon : \mathcal{S}_I \to \{-1, 1\}$ est un morphisme de groupes.

Lemme
Si σ est une permutation de I et $I_1 \cup I_2 \cup .. \cup I_p$ est une partition de I où chaque I_k est σ-stable, alors $\varepsilon(\sigma) = \varepsilon(\sigma_{|I_1})...\varepsilon(\sigma_{|I_p})$.

On vérifie la propriété pour $p = 2$, et on procède par récurrence. On considère sur $I = I_1 \cup I_2$ un ordre total tel que : $\forall x \in I_1 \quad \forall y \in I_2 \quad x < y$. Les inversions de σ sont alors exactement les inversions de $\sigma_{|I_1}$ et celles de $\sigma_{|I_2}$. D´où le résultat.

B- Le décor

Soit n un nombre premier impair. Pour m entier premier avec n ($n \wedge m = 1$), on note $\Pi_{m,n}$ la multiplication par m modulo n (endomorphisme du groupe additif $\mathbb{Z} \setminus n\mathbb{Z}$). Avec le théorème de Gauss, on montre :

$$\forall k \in [[1, n-1]] \quad km \neq 0(n),$$

ce qui fait de $\Pi_{m,n}$ une injection et donc une permutation de $\mathbb{Z} \setminus n\mathbb{Z}$. On a alors au passage, $(n-1)! = m2m...(n-1)m$ d´où : $(m^{n-1} - 1)(n-1)! = 0(n)$ et toujours avec Gauss,

$$m^{n-1} = 1(n) \quad (petit\ théorème\ de\ Fermat).$$

Symbole de Zolotareff vs symbole de Legendre
On définit le symbole de Zolotareff $(m \mid n)$ comme étant la signature de $\Pi_{m,n}$. On a, par exemple, $(-1 \mid n) = (-1)^{\frac{n-1}{2}}$
(décomposer $\Pi_{-1,n} = (1, n-1)(2, n-2)...(\frac{n-1}{2}, \frac{n+1}{2})$, d´où l´équivalence

$$(-1 \mid n) = 1 \Leftrightarrow n \equiv 1(4).$$

Par ailleurs, pour $(m, l) \in \mathbb{Z}^2$, $m \wedge n = 1$, $l \wedge n = 1$, on a : $ml \wedge n = 1$ et $\Pi_{ml,n} = \Pi_{m,n} \circ \Pi_{l,n}$ donc par le morphisme signature, le symbole de Zolotareff est multiplicatif.

On définit le symbole de Legendre $(\frac{m}{n})$ comme suit : $(\frac{m}{n}) = 1$ si m est un carré dans $\mathbb{Z} \setminus n\mathbb{Z}^*$, $(\frac{m}{n}) = -1$ sinon. On remarque que , si m est un carré, le petit théorème de Fermat donne : $(\frac{m}{n}) = m^{\frac{n-1}{2}} = 1$.
On a l´équivalence :

$$(\frac{-1}{n}) = 1 \Leftrightarrow n \equiv 1(4).$$

Une preuve élégante de ce résultat est donné dans RMS-mars-1986 : on envisage sur $\mathbb{Z} \setminus n\mathbb{Z}^*$ la relation d´équivalence $x \Re y \Leftrightarrow y \in \{x, -x, x^{-1}, -x^{-1}\}$, on montre qu´il y a une seule classe à deux éléments (si -1 n´est pas un carré de $\mathbb{Z} \setminus n\mathbb{Z}^*$) ou deux classes à deux éléments (si -1 est un carré), les autres classes au nombre de k ayant 4 éléments ; Cette partition de $\mathbb{Z} \setminus n\mathbb{Z}^*$ donne alors : $n - 1 = 2 + 4k$ ou $n - 1 = 2 + 2 + 4k$...
On rencontre dans RMS-mars-1990 deux relations d´équivalence ("soeurs-jumelles" de $\Re$") qui achèvent la présentation de $(\frac{m}{n})$: $x\mathcal{R}y \Leftrightarrow y \in \{x, x^{-1}\}$ et $x\mathcal{R}_m y \Leftrightarrow y \in \{x, mx^{-1}\}$. Pour $\mathcal{R}$, les classes réduites à un singleton sont $\{-1\}$ et $\{n-1\}$ et dans le produit $(n-1)!$, on regroupe les facteurs par classe, ce qui donne :

$$(n-1)! \equiv -1(n) \quad (théorème\ de\ Wilson).$$

Pour m non carré dans $\mathbb{Z} \setminus n\mathbb{Z}^*$, les classes suivant $\mathcal{R}_m$ ont toutes deux éléments et en regroupant encore une fois les facteurs de $(n-1)!$ par classe, on obtient : $m^{\frac{n-1}{2}} = -1$. En définitive :

$$\forall m \in \mathbb{Z}\ ,\ m \wedge n = 1 \quad (\frac{m}{n}) = m^{\frac{n-1}{2}} \quad (critère\ d'Euler)$$

ce qui assure le caractère multiplicatif du symbole de Legendre.

Lemme de Zolotareff : $(m \mid n) = (\frac{m}{n})$
Deux jolies preuves du lemme sont proposées dans RMS-mars-1990 et RMS-mai-juin-1997. On peut aussi calculer dans le corps $\mathbb{Z} \setminus n\mathbb{Z}$ le symbole $(\frac{m}{n})$ en écrivant : $(\frac{m}{n}) = \prod_{i<j} \frac{mj-mi}{j-i} = \prod_{i<j} m$
d´où : $(m \mid n) = m^{\frac{n(n-1)}{2}} = m^{\frac{n-1}{2}}[m^{\frac{n-1}{2}}]^{n-1}$ et avec le petit théorème de Fermat, $(m \mid n) = m^{\frac{n-1}{2}}$.

Loi de réciprocité quadratique
Pour m et n premiers impairs,

$$(m \mid n)\ (n \mid m) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

C- Définition de Θ et calcul de sa signature

Pour α dans $[[0, nm-1]]$, la division euclidienne de α par m donne l´existence et l´unicité de (i, j) dans $\mathbb{N} \times [[0, m-1]]$ tels que : $\alpha = mi + j$. Par nécessité, i est dans $[[0, n-1]]$. Sinon, $\alpha = mi + j \geqslant mn$. De même, tout entier β de $[[0, nm-1]]$ s´écrit de façon unique : $\beta = nj + i$ avec (i, j) dans $[[0, n-1]] \times [[0, m-1]]$.

Soit Θ l´application de $[[0, nm-1]]$ dans lui-même qui à $\alpha = mi+j$ associe $\beta = nj+i$. Θ est clairement surjective donc Θ est une permutation de $[[0, nm-1]]$.

Lemme : $\varepsilon(\Theta) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$

Preuve expéditive : Avec des notations évidentes,

$$mi + j < mi' + j' \Leftrightarrow i < i' \textit{ ou } [i = i' \textit{ et } j < j']$$

et

$$\Theta(mi + j) > \Theta(mi' + j') \Leftrightarrow j > j' \textit{ ou } [j = j' \textit{ et } i > i'].$$

Les seules inversions de Θ sont donc les couples (i, j) et (i', j') tels que $i < i'$ et $j > j'$, ce qui donne $C_n^2\, C_m^2 = \frac{n(n-1)\, m(m-1)}{2}$ inversions. Le produit nm étant impair, $\varepsilon(\Theta) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$.

Preuve "pédestre" : On commence par partager $[[0, nm-1]]$ en n tranches $T_0, T_1, .., T_n$, T_i désignant la tranche $[[mi, mi+m-1]]$. On remarque que pour tout i dans $[[0, n-1]]$, $\Theta_{|T_i}$ est strictement croissante.

a) Aucune inversion du type (mi, γ).
Si $\gamma > mi$, γ s´écrit : $\gamma = m\tilde{i} + j$ avec $[\tilde{i} = i \textit{ et } 0 < j \leqslant m-1]$ ou $[\tilde{i} > i \textit{ et } 0 < j \leqslant m-1]$. On a : $\Theta(\gamma) = nj + \tilde{i} > \Theta(mi) = i$.

b) $n - 1 - i$ **inversions du type** $(mi+1, \gamma)$.
• Aucune inversion du type $(mi+1, mi+j)$ $\quad (1 < j \leqslant m-1)$ par stricte croissance de $\Theta_{|T_i}$.
• $n - 1 - i$ inversions du type $(mi+1, m\tilde{i})$ avec $i + 1 \leqslant \tilde{i} \leqslant n-1$.
• Aucune inversion du type $(mi+1, m\tilde{i}+j)$ avec $i < \tilde{i} \leqslant n-1$ et $1 \leqslant j \leqslant m-1$. En effet, $\Theta(mi+1) = n + i < \Theta(m\tilde{i}+j) = nj + \tilde{i}$.

On note $I_{i,j}$ le nombre d´inversions du type $(mi+j, \gamma)$ $\quad (1 < j \leqslant n-1)$.

c) On a : $I_{i,j} = (n-1-i)j$

• Aucune inversion du type $(mi+j, mi+\tilde{j})$ avec $j < \tilde{j} \leqslant m-1$.

• Aucune inversion du type $(mi+j, m\tilde{i}+\tilde{j})$ avec $i < \tilde{i} \leqslant n-1$ et $j < \tilde{j} \leqslant m-1$.

• Toutes les inversions de Θ du type $(mi+j, \gamma)$ sont donc parmi les couples $(mi+j, m\tilde{i}+\tilde{j})$ avec $mi+j < m\tilde{i}+\tilde{j}$, $i < \tilde{i} \leqslant n-1$, $0 \leqslant \tilde{j} < j$. On remarque que $(mi+j, \gamma)$ est une inversion dès que $(mi+j-1, \gamma)$ en est une. Ceci donne déjà $I_{i,j-1}$ inversions du type souhaité. Parmi ces $I_{i,j-1}$ inversions, il y a les couples $(mi+j, m\tilde{i}+\tilde{j})$ où $mi+j < m\tilde{i}+\tilde{j}$, $i < \tilde{i} \leqslant n-1$, $0 \leqslant \tilde{j} \leqslant j-2$. En effet, $\Theta(m\tilde{i}+\tilde{j}) = n\tilde{j}+\tilde{i} \leqslant n(j-2)+n \leqslant n(j-1)+i = \Theta(mi+j-1)$ donc $(mi+j-1, m\tilde{i}+\tilde{j})$ est une inversion et il en est de même pour $(mi+j, m\tilde{i}+\tilde{j})$. Enfin, pour tout $i < \tilde{i} \leqslant n-1$, avec $\tilde{j} = j-1$, $(mi+j, m\tilde{i}+j-1)$ est une inversion alors que $(mi+j-1, m\tilde{i}+j-1)$ n´est pas une inversion, ce qui donne $n-1-i$ "nouvelles" inversions. En définitive : $I_{i,j} = I_{i,j-1}+n-1-i$ avec $I_{i,1} = n-1-i$ d´où : $I_{i,j} = (n-1-i)j$.

Le nombre total d´inversions de Θ est : $\sum_{i=0}^{n-1}\sum_{j=0}^{m-1} I_{i,j} = \frac{(m-1)m}{2}\frac{(n-1)n}{2}$. Comme le produit mn est impair, on a : $\varepsilon(\Theta) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

D- Fin de la preuve

Pour $0 \leqslant i \leqslant n-1$ et $0 \leqslant j \leqslant m-1$, on pose :

$$\sigma(i,j) = (mi+j(mod\, n), j) \qquad \tau(i,j) = (i, nj+i(mod\, m)).$$

Avec des notations évidentes, si $\sigma(i_1,j_1) = \sigma(i_2,j_2)$, nécessairement $j_1 = j_2$. On a alors : $m(i_1-i_2) = 0(n)$ et : $i_1 = i_2$ puisque $m \wedge n = 1$. σ, injective, est donc une permutation de $[[0,n-1]] \times [[0,m-1]]$. idem pour τ.

Lemme : $\varepsilon(\sigma) = (m \mid n) \qquad \varepsilon(\tau) = (n \mid m)$.

$\bigsqcup_{0\leqslant j\leqslant m-1} [[0,n-1]] \times \{j\}$ est une partition de $[[0,n-1]] \times [[0,m-1]]$ où chaque $[[0,n-1]] \times \{j\}$ est σ-stable donc d´après le lemme de la partie A :

$$\varepsilon(\sigma) = \prod_{0\leqslant j\leqslant m-1} \varepsilon(i \mapsto mi+j) = \prod_{0\leqslant j\leqslant m-1} \varepsilon(\Pi_{m,n})\varepsilon(t_j : i \mapsto i+j).$$

Or, pour $0 \leqslant j \leqslant m-1$, t_j est la puissance $j^{ème}$ du n-cycle $x \mapsto x+1$ donc $\varepsilon(t_j) = (-1)^{(n-1)j} = 1$ car n est impair. Ainsi, $\varepsilon(\sigma) = (m \mid n)^m$ et comme m est impair, $\varepsilon(\sigma) = (m \mid n)$. De même : $\varepsilon(\tau) = (n \mid m)$.

Dernière étape

Reste à relier σ et τ. Soit Ch la bijection $x(mn) \mapsto (x(n), x(m))$ de $\mathbb{Z} \setminus mn\mathbb{Z}$ sur $\mathbb{Z} \setminus n\mathbb{Z} \times \mathbb{Z} \setminus m\mathbb{Z}$ (isomorphisme d´anneaux).

On a : $Ch(mi+j) = (mi+j, j)$ et : $Ch(nj+i) = (i, nj+i)$

donc : $\Theta = Ch^{-1} \circ \tau \circ \sigma^{-1} \circ Ch$. De là : $\varepsilon(\Theta) = \varepsilon(\sigma)\varepsilon(\tau)$ c.a.d :

$$(-1)^{\frac{n-1}{2}\frac{m-1}{2}} = (n \mid m)(m \mid n).$$